Notice of Allowability	**Application No.** 10/001,687	**Applicant(s)** BUSHMITCH ET AL.
	Examiner Kaveh Abrishamkar	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the after-final amendment filed on 12/13/2006*.

2. ☒ The allowed claim(s) is/are *1-10,24-42,46-56 and 59-67*.

3. □ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) □ All b) □ Some* c) □ None of the:
   1. □ Certified copies of the priority documents have been received.
   2. □ Certified copies of the priority documents have been received in Application No. _____ .
   3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. □ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. □ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) □ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) □ hereto or 2) □ to Paper No./Mail Date _____.
   (b) □ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. □ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. □ Notice of References Cited (PTO-892)
2. □ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. □ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. □ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. □ Notice of Informal Patent Application
6. □ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. □ Other _____.

CHRISTOPHER REVAK
PRIMARY EXAMINER

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

2. Authorization for this examiner's amendment was given in a telephone interview with Timothy MacIntyre (Registration No. 42,824) on January 3, 2007.

3. The application has been amended as follows:

4. Claims 17-23 are cancelled by virtue of this Examiner's Amendment.

5. Claim 40 (Currently Amended):

A security method comprising:

storing a set of N password-key pairs in a gateway device situated between a trusted network and an untrusted network, N being an integer greater than one;

storing a set of N encrypted values in a portable storage device;

placing the portable storage device in communication with a remote client;

communicating between the remote client and the gateway device via the untrusted network;

sending a password-specific~~-~~_key_of one of said set of password-key pairs to the remote client;

requesting an identification value from a user of the remote client;

creating a combination of said identification value and said password-specific key;

decrypting a corresponding encrypted value from said set of encrypted values using said combination;

transmitting a result of said decryption to the gateway device;

authenticating the remote client if said result is equal to a password of said one of said set of password-key pairs;

further comprising requesting said identification value from the user, and wherein said generating includes generating said set of encrypted values from said identification value and said set of password-key pairs~~.~~;

wherein said generating includes generating each of said set of encrypted values by encrypting a respective password of said set of password-key pairs with a combination of a respective key of said set of password-key pairs and said identification value~~.~~;

wherein said generating includes encrypting said identification value with a symmetric key~~.~~;

further comprising storing the symmetric key in a protected area of the portable storage device that is only accessible upon authentication of the portable storage device; and

encrypting the identification value with the symmetric key stored on the portable device prior to said creating the combination, said decrypting, and said transmitting.

Claim 46 (Currently Amended):

The method of Claim ~~45~~40 wherein said generating includes combining said encrypted identification value with said respective key using a bitwise exclusive-or.

Claim 56 (Currently Amended):

A gateway device situated between a trusted network and an untrusted network, comprising:

a firewall module that restricts access to the trusted network;

a storage module that stores a set of N password-key pairs, N being an integer greater than one;

an initialization module that generates said set of password-key pairs, requests an identification value from a user, generates a set of N encrypted values from said set of password-key pairs and said identification value, and is capable of communicating said set of encrypted values to a portable storage device when the portable storage device is in secure communication with said gateway device; ~~and~~

an authentication module that sends a password-specific key of one of said set of password-key pairs to a remote client over the untrusted network, receives a decryption result from the remote client, and authenticates the remote client if said decryption result is equal to a password of said one of said set of password-key pairs;

wherein said initialization module generates each of said set of encrypted values by encrypting a respective password of said set of password-key pairs with a combination of a respective key of said set of password-key pairs and said identification value~~.~~;

wherein said combination of said respective key and said identification value includes a function of said identification value encrypted with a symmetric key and said respective key; and

wherein said initialization module stores the symmetric key in a protected area of the portable storage device that is only accessible upon authentication of the portable storage device.

Claim 59 (Currently Amended):

The gateway device of claim ~~58~~56 wherein said function is a bitwise exclusive-or.

REASONS FOR ALLOWANCE

1. Claims 1-10, 24-42, 46-56, and 59-67 are allowed.

2. The following is an examiner's statement of reasons for allowance:

3. The above-mentioned claims are allowable over the prior art because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in

combination with the specific added limitations by virtue of the after-final amendment, as recited in independent claims 1, 24, 40, and 56, and the subsequent dependent claims.

The CPA does not explicitly teach nor suggest a method, system, or device which comprises a gateway device which sends a password-specific to a portable storage device, wherein the password is retrieved by decrypting an encrypted value using a combination of a encrypted identification value and the password specific key by using the process described in the independent claims 1, 24, 40, and 56.

4. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

K.A. 1/4/07
KA
01/04/2007

CHRISTOPHER REVAK
PRIMARY EXAMINER